LA VANGUARDIA

LA PRIVACIDAD EN INTERNET

Ya no vale todo con nuestros datos personales

A partir del 25 de mayo el Reglamento de Protección de Datos es de obligado cumplimiento en toda la UE

La información personal de los usuario de internet gozará de una mayor protección a partir del 25 de mayo (Colin Anderson / Getty)

ALBERT MOLINS RENTER, Barcelona
11/05/2018 01:56 | Actualizado a 11/05/2018 08:38

Aunque ya lleva casi dos años en vigor, a partir del próximo 25 de mayo el **Reglamento de Protección de Datos** (RGPD) pasa a ser de **obligado cumplimiento**. Lo primero que hay que entender es que el **RGPD** no es un instrumento de censura y que, por tanto, su ámbito de aplicación no son los contenidos. El reglamento no está pensado para luchar contra las *fake news* ni para evitar la pornografía infantil en la red. Ni tan siquiera está pensado para luchar contra el cibercrimen. Se trata de una norma destinada a evitar que nuestra **información personal** circule fuera de control en **internet**. Y lo más importante es que introduce un **marco regulatorio común** para todos los países de la **UE**.

Esta era una demanda de muchas empresas del sector tecnológico, ya que hasta ahora tenían que hacer frente a 28 legislaciones diferentes. Uno de los principios en los que se basa el RGPD es que la protección de los datos de los ciudadanos de la UE debe ser proactiva, y por eso el reglamento implementa la privacidad por diseño, que implica que cuando se diseña o programa una aplicación o página web, hay que hacerlo incorporando en su planificación las medidas de protección de la privacidad necesarias.

Estos son aquellos aspectos del nuevo marco regulatorio europeo que tienen una mayor importancia en nuestro día a día en la red:

El problema: la hiperconectividad

Ya no es sólo el teléfono inteligente, ahora todo se conecta a internet. Relojes, electrodomésticos, peceras, hervidores de arroz y hasta nuestro coche recogen datos y los mandan no sabemos muy bien dónde y, lo que es peor, no sabemos muy bien para qué. Esta hiperconectividad potencialmente podría convertirse en "la responsable de que perdamos el control de quién recoge y con qué finalidad nuestros datos", explica Albert Agustinoy, socio responsable del área de propiedad intelectual y nuevas tecnologías del bufete Cuatrecasas. "Por ejemplo, en un reloj inteligente, ¿quién recoge nuestros datos?¿El fabricante, el desarrollador de la aplicación?", se pregunta Agustinoy. Por eso una de las primeras cuestiones de las que se ocupa el RGPD es de cómo otorgamos nuestro consentimiento sobre la recogida y el procesamiento de nuestra información personal.

Qué son datos personales

Se entienden como tales, cualquier información relacionada con una persona que pueda usarse para identificarla, incluyendo su nombre, fotos, dirección de correo electrónico, dirección IP, datos bancarios, publicaciones en sus redes sociales, información médica, datos biométricos y su orientación sexual.

El consentimiento

Primero estampábamos nuestra firma en una hoja de papel, de la que nos llevábamos una copia en papel carbón. "Luego fue mediante un clic, y actualmente ni eso", dice Agustinoy. Muchas veces con sólo navegar por un página web o por usar una aplicación ya estamos dando permiso para que se guarden y usen nuestros datos personales. Cuando compramos un nuevo dispositivo conectado, todos lo que queremos es empezar a usarlo lo antes posibles, pero con la entrada en vigor del RGPD "será exigible que para cualquiera de estos wearables o dispositivos se creen unos hábitos de activación que llamen la atención e informen de forma efectiva a los usuarios de que sus datos serán recogidos y de cómo serán utilizados. Que nos informen de que esa información acabará en unos servidores que están en EE.UU. –por ejemplo– y que se compartirán con otra empresa cuyos servidores están en China".

Hay que recordar que según el artículo 3 del RGPD si una compañía ofrece sus servicios en cualquier país miembro de la UE, no importa en qué lugar almacene los datos, debe cumplir con el reglamento. Por eso, según Albert Agustinoy, el gran reto que plantea el RGPD a los fabricantes y a cualquiera que recopile información privada de sus usuarios "es como consiguen un consentimiento efectivo, que el RGPD define como un consentimiento informado, explícito y previo, cuando lo que queremos es poner en marcha aquel dispositivo lo antes posible".

Agustinoy cree que el sistema de consentimiento previsto en el RGPD no soluciona totalmente esta difícil cuestión. "Aunque el sistema por capas ya es un avance, en muchas ocasiones el cumplimiento de la norma conducirá a una cláusula informativa larga y compleja, lo cual puede conducir al resultado de que nadie termine leyéndola. Simplificar y centrarse en las cuestiones previstas por el reglamento será clave", opina el socio de Cuatrecasas.

El derecho de acceso

Además, de más información previa sobre qué se recogerá, cómo se recogerá y quién lo almacenará, el derecho de acceso es el que "garantiza a los ciudadanos que las empresas utilizan los datos para aquello que nos han dicho que los utilizarán", dice Agustinoy. El reglamento confirma nuestro derecho a preguntar a las empresas que nos digan qué categorías de datos tienen sobre nosotros

Si un empleado presenta una solicitud de acceso, su empleador tendrá 30 días para recopilar toda la información almacenada sobre él. Esto podría incluir potencialmente menciones a informes de rendimiento, entrevistas de trabajo, registros de nómina, registros de ausencia, registros disciplinarios, registros de acceso al ordenador, secuencias de circuitos cerrados de televisión y grabaciones de llamadas telefónicas.

El derecho de acceso es anterior al RGPD, pero ahora se facilita su ejercicio reduciendo el tiempo de respuesta de 40 días a 30 días y con la introducción de sanciones duras para las empresas que no cumplan.

La única cuestión aquí es que siempre será a posteriori. El RGPD no establece ningún organismo ni ningún mecanismo que controle que realmente las empresas recogen sólo los datos sobre los que el usuario ha dado su consentimiento y que los usa exclusivamente para lo que el usuario ha dado permiso. Entonces, ¿qué garantiza que esto se cumpla? Según Agustinoy, "las compañías se la juegan con una responsabilidad del 4% de su volumen de negocio o de 20 millones de euros", que son las sanciones máximas que establece el RGPD.

Derechos expandidos para el consumidor

Además, la nueva regulación de protección de datos incluye nuevos derechos que hasta ahora no estaban recogidos. Concretamente el derecho al olvido, lo que significa que las empresas deben eliminar los datos de una persona si esta retira su consentimiento para que la empresa los tenga. Pero hay casos en los que la práctica no es tan fácil. Por ejemplo, si está en vigor una relación contractual o existe un plazo legal de conservación, como puede ser mantener los datos fiscales a disposición de la Agencia Tributaria.

La portabilidad permite que, si nuestros datos se están tratando de manera automatizada, los podamos recuperar para cederlos a otra empresa. Estos datos deben estar en un formato estructurado, de uso común y lectura mecánica (por ejemplo un excel) para que se puedan transmitir fácilmente a otro responsable y facilitar, por ejemplo, un cambio de proveedor.

También se establece con claridad a quién debemos reclamar en caso de que creamos que se han infringido nuestro consetimiento, y nos otorga el derecho a oponernos a un uso específico de nuestra información mientras se resuelve una reclamación. Por último, establece un sistema de compensación para el afectado. La posibilidad de que, una vez exista la constatación de una infracción, reclamar una compensación.

Menores

Estos días se ha dicho y escrito que con la entrada en vigor del RGPD, los menores de 16 años tendrán prohibido el uso de aplicaciones como WhatsApp. No es cierto. Lo único que establece esta nueva norma es la edad en la que una persona puede otorgar su consentimiento por sí sola. Para los menores de 16 años, WhatsApp –para seguir con el mismo ejemplo– deberá obtener el consentimiento de los padres del menor, tal y como se recoge en los términos de uso de la aplicación.

Una vez obtenido, cualquier menor de esta edad puede tener instalada la aplicación de mensajería en su teléfono y usarla sin ninguna restricción. Otra cosa es que WhatsApp realmente pida a los padres que den el consentimiento en nombre de sus hijos.

Según Mònica Vilasau, profesora de los Estudios de Derecho y Ciencia Política de la UOC, se trata de una medida "difícilmente aplicable", ya que es muy complicado establecer mecanismos que permitan saber con certeza la edad de una persona. "Es obvio que cualquier chico más joven de dieciséis años puede recurrir a otro mayor para que lo ayude, o bien puede buscar en internet alguna estrategia para conseguir registrarse", explica. Tiene una visión muy parecida a Mireia Montaña, profesora de los Estudios de Ciencias de la Información y de la Comunicación de la UOC, que apunta que "si el único control es preguntar a los usuarios qué edad tienen, no funcionará: los niños y los jóvenes mentirán con el fin de poder seguir utilizando la aplicación", razona. Por su parte Albert Agustinoy cree que no sería imposible que WhatsApp implementara mecanismos para obtener el consentimiento paterno, que podrían ir "desde enviar un sms al teléfono de los padres o sistemas basados en inteligencia artificial", pero también tiene sus dudas de la futura aplicación de medidas como las indicadas.

Vilasau cree que "la protección de los derechos de los menores en internet sólo es posible si no utilizan los móviles, no publican ningún tipo de contenidos en internet ni están dados de alta en ninguna red social", asegura. Sin embargo, esta experta dice que eso es imposible en una sociedad tan digitalizada como el actual, en que los menores ya han crecido con las nuevas tecnologías.

Ambas expertas de la UOC coinciden en el hecho de que lo más efectivo con vistas al uso de este tipo de aplicaciones es educar en el uso de las nuevas tecnologías. Y eso sí, "la medida adoptada por WhatsApp puede servir para que los padres y las madres de menores sean más conscientes de la trascendencia que tiene el uso de las aplicaciones móviles y las redes sociales de manera habitual y continua por parte de los menores, y que de alguna manera eso les lleve a supervisar mejor el uso que hacen sus hijos", asegura Vilasau.

Cómo reclamar

Como es lógico el reglamento se aplica a los 28 estados miembros y como principio general se aplica un sistema de ventanilla única para presentar una reclamación. Si por ejemplo, creemos que Facebook está haciendo un uso indebido de nuestros datos, hay que presentar la denuncia ante la agencia irlandesa de protección de datos, que es donde Facebook tiene su sede en Europa. Se puede presentar ante la Agencia Española de Protección de Datos (AEPD), "pero, en principio, ésta lo que tendrá que hacer es enviarla a Irlanda", dice Agustinoy.

Esto funciona así menos en el caso de la llamada excepción de vinculación nacional. “Si se trata de un caso que sólo afecta a nacionales de un estado miembro, de una actividad que sólo se ofrece a ciudadanos de aquel país, entonces sí que la agencia que haya recibido la queja la podrá gestionar pidiendo permiso a la que le tocaría según el principio general”, explica el socio de Cuatrecasas.

Un caso de este tipo sería, por ejemplo, el de “un sitio de juego online, que opera en España bajo una licencia otorgada por el Ministerio de Hacienda, bajo un dominio .es y en el que sólo se pueden registrar ciudadanos españoles. En este caso, aunque el operador esté en Reino Unido, sería competencia de la AEPD”, apunta Agustinoy.

Una vez presentada la reclamación, la AEPD comunica que ha iniciado un procedimiento sancionador, y si finalmente hay sanción, con la resolución de la AEPD, el ciudadano podrá presentar una denuncia a los tribunales ordinarios.

Informar en caso de una brecha de seguridad

Cuando se produzca un ciberataque en el que se haya producido un robo de datos personales, el RGPD impone un plazo de 72 horas (a contar desde su detección) para que la empresa comunique que ha sufrido un incidente de seguridad, y no sólo deberá informar a las autoridades, sino también a todos aquellos que se hayan podido ver afectados.

Deberes

También se ha dicho que el RGPD limitaba la posibilidad de mandar correo, por ejemplo para organizar una fiesta de cumpleaños, o de meter a alguien sin su consetimiento en un grupo de WhatsApp, o de subir a la red las fotos de una boda. Tampoco es cierto.

“El uso genuinamente doméstico de datos está exento de la aplicación del RGPD, porque en este tipo de actividades no hay un afán de explotación de estos datos”, asegura Agustinoy. De todos formas, este abogado cree que “como usuarios también tendremos que hacer una transición y tenemos que ser conscientes del uso que hacemos de redes sociales y aplicaciones y configurar nuestros perfiles al grado de exposición que consideremos adecuado”.

Y es que el reglamento, en definitiva y aunque pueda parecer paradójico, trata de proteger la información personal de unos individuos que de forma voluntaria cada vez sobreexponen más su propia intimidad en la red.